Symantec High Availability Solution- Support for VMware SRM

Windows Server 2008 (x64), Windows Server 2008 R2 (x64)

6.0.1

November 2012

Contents

Chapter 1

Introduction

This chapter includes the following topics:

About the Symantec High Availability Solution

The Symantec High Availability solution for VMware employs Veritas Cluster Server (VCS) and its agent framework to monitor the state of the applications and their dependent components running on the virtual machines, configured in a protection group. These virtual machines use non-shared storage. Specific agents are available to monitor the application, storage, and network components. Together, these agents monitor the overall health of the configured applications by running specific commands, tests, or scripts.

The storage configuration in the VMware virtual environment determines how VCS functions differently in a non-shared virtual environment. The non-shared storage configuration in the VMware virtual environment involves the VMware VMDK and RDM disks that reside on the shared datastore. This datastore is accessible to multiple virtual machines. However, the disks are attached to a single virtual machine at any given point of time.

VCS provides a new storage agent “VMwareDisks” that communicates with the VMware ESX/ESXi hosts to perform the disk detach and attach operations to move the storage disk between the virtual machines, in a VCS cluster.

Note: For application monitoring continuity in a VMware SRM environment, you must configure the VCS cluster communication links using the MAC address (LLT over Ethernet option). If you use IP address (LLT over UDP option) to configure the cluster communication links, then the VCS cluster fails to start after the virtual machines are failed over to the recovery site.

To configure application monitoring in a site recovery environment, Symantec High Availability solution additionally provides script files for the following tasks:

- Set up communication between the vCenter Server and the SRM Server at the recovery site and the virtual machines at the protected site.
- Assign a SiteID to both the sites.
- Specify attribute values for the application components at the respective site.
- Retrieve the application status in the SRM recovery report, after the virtual machine is started at the recovery site.

These files are invoked when the SRM recovery plan is executed.

In event of an failure in a local site configuration, the following tasks are performed for application monitoring continuity:

- The VCS agents attempt to restart the application services and components for a configurable number of times.
- If the application fails to start, they initiate an application fail over to the failover target system.
- During the fail over, the VMwareDisks agent moves the storage disk to the failover target system, the network agents bring the network components online, and the application-specific agents then start the application services on the failover target system.

In event of a failure in a site recovery configuration, the following tasks are performed for application monitoring continuity:

- The virtual machines at the protected site are failed over to the recovery site.
- The pre-online script defined in the form of a command in the SRM recovery plan applies the specified attribute values for the application components.
- The status monitoring script retrieves the application status.
- The network agents bring the network components online and the application-specific agents start the application services on the failover target system.

Note: The Symantec High Availability Dashboard fails to remove the application details, if you unconfigure application monitoring after the application is failed over to the recovery site. Even after application monitoring is unconfigured the Dashboard continues to display the stale records.

Supported VMware SRM versions

The Symantec High Availability solution currently supports the VMware SRM Server version 5.0, 5.1 and 5.1.0A.

Chapter 2

Deploying the Symantec High Availability Solution

This chapter includes the following topics:

About deploying the Symantec High Availability Solution in VMware SRM environment

You can deploy the Symantec High Availability Solution in a VMware SRM environment by performing the following tasks:

Verify the pre-requisites	Review the pre-requisites before you begin to deploy the Symantec High Availability Solution in VMware SRM environment. See "Prerequisites" on page 12.
Replace the ac.war file on the recovery site ApplicationHA Console	Replace the existing ac.war file with the one provided with this patch See "Replacing the ac.war file" on page 14.
Configure SSO between the Symantec High Availability Console at the recovery site and the protection group virtual machines (at the protected site)	The SSO configuration enables communication between the protected site virtual machines, and the recovery site Symantec High Availability Console. This configuration maintains continuity between the virtual machine and Console communication even after failover. See "Configuring SSO between the protected and the recovery site" on page 15.
Copy the provided script files	Copy the following script files to invoke or execute various functions. You must copy these files at the specified location. ■ getAppStatus.pl ■ getAppStatus.bat ■ preonline.pl ■ setSiteID.ps1 See "Copying the script files" on page 13.
Update the SRM recovery plan	Modify the SRM recovery plan to define the action for application monitoring continuity. See "Updating the SRM recovery plan" on page 18.

Encrypt the recovery site vCenter Server password	This is an optional task. Execute the `EncryptvCenterPassword.ps1` script to encrypt the recovery site vCenter Server password. You must perform this task only if you plan to set up the communication with the recovery site vCenter Server, using the encrypted password . Alternatively, you can configure the "VMware vCenter Site Recovery Manager Server" service or then provide the vCenter Server password in the command that needs to be added to the SRM Recovery Plan. See "Encrypting the recovery site vCenter Server password" on page 16.
Encrypt the recovery site ESX password	Use the vcsencrypt utility to encrypt the recovery site ESX password. You need to specify this encrypted password in the VCS_Site_Info.xml See "Encrypting the ESX password" on page 20.
Modify the attributes for the application components	Update the attribute values in the VCS_Site_Info.xml. This file lists the attributes and their corresponding values for the application components. The attributes and their values must be specified for both, the protected and the recovery site. See "Modifying the attributes for the application and its component dependency group" on page 21.
Configure the "VMware vCenter Site Recovery Manager Server" service	This is an alternative task. You must perform this task only if you have not executed the `EncryptvCenterPassword.ps1` script but plan to encrypt the secondary site vCenter Server password. You can configure the "VMware vCenter Site Recovery Manager Server" service only if the SRM Server and the vCenter Server are present in the same domain. You must perform this tasks before you execute the recovery plan. See "Configuring the SRM service " on page 17.

Prerequisites

Review the following pre-requisites before you begin to deploy the Symantec High Availability Solution in VMware SRM environment:

Set up the VMware SRM environment	Ensure that you have performed the following tasks while you set up the SRM environment: ■ Install and configure VMware SRM and vCenter Server at both, the primary and the recovery site ■ At the protected site, set up a protection group for the virtual machines on which you want to configure appliaction monitoring ■ Create a SRM recovery plan ■ In the SRM recovery plan, verify if the virtual machines in the protection group are included in the same priority group. This required to ensure that all the virtual machines in a VCS cluster are failed over at the same time. ■ Install the vSphere PowerCLI on the SRM Servers. For more details on performing each of these tasks, refer to VMware product documentation.
Install Symantec High Availability Console	Ensure that the Symantec High Availability Console is installed at both, the protected and the recovery site. For more details refer to, *Symantec High Availability Console Installation and Upgrade Guide*.
Install the Symantec High Availability Guest Components	Install VCS or SFW HA, as part of the Symantec High Availability guest components installation. Install these components on all the virtual machines (at the protected site) where you want to configure application monitoring. These virtual machines must be a part of the protection group. For details refer to the *Symantec High Availability Solutions Guide for VMware*.
Configure SSO	Configure SSO between the Symantec High Availability Console and the guest machine on the respective sites. For more details refer to *Symantec High Availability Solutions Guide for VMware*.

Verify that the user account privileges and the ports are enabled	■ The vCenter logged-on user must have the Symantec High Availability administrator privileges on the virtual machines at the protected site. ■ The https port used by the VMware Web Service is enabled for inbound and outbound communication. The default port is 443. ■ The https port used by Veritas Storage Foundation Messaging Service (xprtld) is enabled for inbound and outbound communication. The default port is 5634. ■ Ports 5634, 14152, and 14153 are not blocked by a firewall on the Console hosts and the virtual machines.
Verify if the required services are running on the Symantec High Availability Console at both the sites	■ Symantec ApplicationHA Service (ApplicationHA Console) ■ Veritas Storage Foundation Messaging Service (xprtld) ■ Symantec Authentication Service
Others	■ Ensure that the virtual machines can access the Console host at both the sites. ■ Ensure that the virtual machines can access the Console host at recovery site using the fully qualified host name. ■ Ensure that the clock times on the protected site virtual machines and the recovery site ApplicationHA Console are within 30 minutes of one another.
Configure application monitoring	At the protected site, ensure that application monitoring is configured on the virtual machines and the VCS cluster is formed. For more details on configuring application monitoring, refer to the respective application configuration guides. **Note:** For application monitoring continuity in a VMware SRM environment, you must configure the VCS cluster communication links using the MAC address (LLT over Ethernet option). If you use IP address (LLT over UDP option) to configure the cluster communication links, then the VCS cluster fails to start after the virtual machines are failed over to the recovery site.

Copying the script files

This patch provides the following files/scripts to invoke or execute various functions. You must copy these files at the specified location on the recovery site SRM Server or the local virtual machine.

To copy the scripts/files download and extract the patch zip file to a temporary location on your system. Access the temporary location and then copy the respective file to the location as that specified in the following table:

getAppStatus.pl	This script retrieves the application status after it is started at the recovery site. Copy this script on all the virtual machines at the following location: %vcs_home%\portal\admin
getAppStatus.bat	This file executes the getAppStatus.pl script. Copy this script on all the virtual machines at the following location: %vcs_home%\bin
preonline.pl	This script executes the vcs_site_info.xml and applies the specified attribute values for the respective site. Copy this script on all the virtual machines at the following location: %vcs_home%\bin\Triggers
setSiteID.ps1	This script applies or assigns a SiteID to both the sites. Copy this script to a temporary location on the SRM Server at the recovery site. This script is executed when the command specified in the Pre-power On Step of a virtual machine is run.

Replacing the ac.war file

Before you configure single sign-on between the recovery site ApplicationHA Console and the virtual machines at the protected site you must replace the ac.war file from the recovery site Console Server.

Perform the following steps to replace the ac.war file

Note: You must perform these steps from the recovery site ApplicationHA Console.

---

1. Copy the ac.war file that is provided with this patch and save it at any temporary location.
2. From the Windows services panel, stop the ApplicationHA service.

3 Navigate to the following location:

   `InstallDirectory\ApplicationHA\webapp\`

   Where,

   InstallDirectory is path that you had selected while installing the ApplicationHA Console.

4 Copy the saved ac.war file and replace the existing file.

5 From the Windows services panel, start the ApplicationHA service.

Configuring SSO between the protected and the recovery site

Use the Symantec ApplicationHA SRM Components Configuration Wizard to configure the single sign-on between the protected and recovery site. You must launch this configuration wizard from the Symantec High Availability Console at the recovery site.

To configure the single sign-on

1 On the recovery site, using the vSphere Client, connect to the vCenter Server and navigate to **Home** > **Solutions and Applications** > **Symantec High Availability**.

2 On the Symantec High Availability home page, click the **Disaster Recovery** tab.

3 On the Disaster Recovery tab, click **Configure Single Sign-on**.

   This launches the Symantec ApplicationHA SRM components configuration wizard.

4 Review the prerequisites on the Welcome panel and then click **Next**.

5 On the ApplicationHA Inputs panel, specify the required details of the Symantec High Availability Console and the vCenter Server at the protected site.

   The wizard uses these details to set up a link with the protected site virtual machines and the Symantec High Availability Console at the recovery site. This link enables communication with the guest virtual machines at the protected site.

6 On the System Selection panel, select the virtual machines for configuring single sign-on.

7 The Implementation panel displays the SSO configuration progress for each virtual machine. After the configuration process is complete, click **Next**.

If the configuration has failed on any of the machine, refer to the log files for details.

The log file is located on the protected site Symantec High Availability Console at the following location:

```
%AllUsersProfile%\Symantec\ApplicationHA\Logs
```

You may have to rectify the cause and repeat the configuration on the failed machines.

8 On the Finish panel, click **Finish**.

This completes the SSO configuration between the virtual machines at the protected site and the Symantec High Availability Console at the recovery site.

Encrypting the recovery site vCenter Server password

This is an optional task.

You must perform this task only if you plan to encrypt the recovery site vCenter Server user account password (that is; if you do not want to specify the vCenter Server user account password in the command step that must be added to the SRM Recovery Plan for application monitoring continuity).

Alternatively, you can avoid providing the password in the command step by configuring the VMware vCenter Site Recovery Manager Server service (only if the SRM Server and the vCenter Server are in the same domain).

The EncryptvCenterPassword.ps1 script stores the vCenter Server user account credentials at a specified or the default location. These details are then used by the command step that you add to update the recovery plan.

To encrypt the vCenter Server user account password

1. Copy the EncryptvCenterPassword.ps1 script to a temporary location on the SRM Server at the recovery site.
2. From the command prompt run the following command:

   ```
   C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   -ExecutionPolicy Unrestricted c:\encryptVCenterPasswd.ps1 [-
   CredPath]
   ```

   Where,

   CredPath is the path where you want to save the vCenter Server user account credentials. For example, *c:\users\administrator\VCenterUserInfo.xml*

   Note: Ensure that the path is specified in ‘ ‘ (single quotes) and that it does not contain the character ‘&’ in it.

   The encryptVCenterPasswd.ps1 script fails to save the vCenter Server user account details at a specified path, if the path is specified in “ “ (double quotes) and contains a space. Also, if the path contains a character ‘&’ in it the script displays an error indicating that the specified path does not exists.

   If you do not specify the FileName, then the user account credentials are saved at the following location by default:

   `C:\ProgramData\VCenterUserInfo.xml` is used.

   After you run the command, a dialogue box to specify the vCenter Server user account details is displayed.

Configuring the SRM service

This is an alternative task.

You must perform this task only if you have not executed the EncryptvCenterPassword.ps1 script, but want to encrypt the secondary site vCenter Server user account password (do not want to specify the vCenter Server user account password in the command step to be added to the recovery plan).

You can configure the "VMware vCenter Site Recovery Manager Server" service only if the SRM Server and the vCenter Server are present in the same domain.

Perform this task before you execute the recovery plan.

To configure the SRM service

1. On the SRM Server at the recovery site, launch the Windows Services panel.
2. Select and double-click on the "VMware vCenter Site Recovery Manager Server" service.
3. On the service dialog box that appears, select the **Log On** tab.
4. On the Log On tab, select **This account** and browse or specify the vCenter Server user account details.
5. Click **Ok**.

Updating the SRM recovery plan

After you have configured SSO between the recovery site Symantec High Availability Console and the protected site virtual machines, you must modify the SRM recovery plan to define the action for application monitoring continuity. This action is defined in the form of an Symantec High Availability recovery command that must be added to the SRM recovery plan.

Note: You must perfom these steps on all the virtual machines.

To update the SRM recovery plan

1. Using the vSphere Client, navigate to **Home** > **Solutions and Applications** > **Site Recovery**

   In the left pane, select **Recovery Plan**.
2. From the list of recovery plans, select the recovery plan to be updated.
3. In the recovery plan, select the virtual machine, right-click and click **Configure**.
4. On the VM Recovery Properties panel, select **Pre-power On Steps** in the left pane and click **Add** in the right pane.
5. On the Add Pre-power On Step panel, perform the following tasks:
   - Select **Command on SRM Server**
   - In the Name text box, specify a name for the command step to be added
   - In the Content text box, specify the following command

     ```
     C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
     -ExecutionPolicy Unrestricted c:\setSiteID.ps1 -vCenter <IP address>
     -SiteId <ID> -VM 'VirtualMachine HostName'
     ```

```
-U Administrator -P Password
-UseFileCred 0/1
-CredPath CredFilePath
```

Where,

- IP address = The IP address of recovery site vCenter Server. If you do not specify the IP address, then the vCenter Server hostname is considered by default.
- ID= Specify an ID for the recovery site
  This is required when you modify the vcs_site_info.xml file.
  If you do not specify an ID, the hostname of recovery site SRM Server is used.
- VirtualMachine HostName= Host name of the local machine as that specified in the vCenter server inventory

  Note: Ensure that the hostname does not contain any special characters. If the hostname contains any special characters, then the "setSiteID.ps1" script that is used to assign a site ID to the respective sites fails to assign these IDs.

- Administrator= User account name for the recovery site vCenter Server
- Password= Password for the user account specified
- UseFileCred= Specify a value for this argument depending on whether or not you have encrypted the vCenter Server user account password, using the encryptVCenterPassword.ps1 script.
  0= The vCenter Server password is not encrypted and you need to specify the password in the command.
  1= The vCenter Server password is encrypted and is saved at a temporary location.

  Note: You need not specify this argument if you plan to configure the SRM service. This service configuration helps to automatically establish a connection with the vCenter Server.

- CredFilePath= File path where the vCenter Server user account credentials are saved
  You need to specify this variable only if you have specified '1' for UseFileCred variable.

Note: User account details are required only if you intend to encrypt the vCenter Server user account password. To encrypt the password, you must execute the EncryptvCenterPassword.ps1 script. This script saves the user account details at the specified or default location. The CredPath specified is applied only if the UseFileCred argument value is 1.

- Click **Ok**.

6 On the VM Recovery Properties panel, from the left panel, select **Post Power On Steps** and click **Add**.

7 On the Add Post Power On Step panel, perform the following:

- Select **Command on Recovered VM**
- In the Name text box, specify a name for the command step to be added
- In the Content text box, specify the following command step

  ```
  "%vcs_home%\bin\getAppStatus.bat"
  ```

  This script retrieves the application status after it is started at the recovery site.
- Click **Ok**.

Encrypting the ESX password

Before you specify passwords in the XML configuration file, you must encrypt them by using the vcsencrypt utility.

Perform these steps for all the passwords to be specified in the XML file.

To encrypt a password

1 Run the vcsencrypt utility by typing the following on the command line.

```
C:\> vcsencrypt -agent
```

2 The utility prompts you to enter the password twice. Enter the password and press **Enter**.

```
Enter New Password:

Enter Again:
```

3 The utility encrypts the password and displays the encrypted password.

4 Specify this encrypted password in the XML file.

Modifying the attributes for the application and its component dependency group

The VCS_Site_Info.xml file saves a site ID for both, the protected and the recovery site. It also lists the attributes for the configured application components. Each attribute must have a corresponding value on both the sites.

During a disaster, when the virtual machines fail over to the recovery site, VCS considers these attribute values and then starts the application.

Note: You must perform this task on all the virtual machines that are a part of the protection group.

To modify the attribute values

1. Copy the vcs_site_info.xml file and save it to the following location on a virtual machine in the protection group:

   %VCS_Home%\conf

2. Modify the xml file to specify a SiteID for the protected and the recovery site. Also, update the required resource names and attribute values for the respective sites.

   Note: Ensure that the specified attribute values do not contain any of these special characters ", < and >". If the attribute values contain any of these characters, then the preonline.pl script fails to appliy the specified attributes to the respective sites.

   ---

3. Copy and save this modified XML file on all the virtual machines.
4. Using the VCS Java Console, perform the following tasks:
   - Select the application dependency group and set its "PreOnline Trigger" attribute to "True".
   - Ensure that the "AutoStartList" attribute includes all the virtual machines that were specified in the Failover Target System List of the application dependency group.

     Note: You must perform this step for each application dependency group from any virtual machine in the protection group.

Appendix A

Test failover configuration

This appendix includes the following topics:

About executing the test recovery plan

After you have configured the sites for disaster recovery, you can test the recovery plan to verify the fault-readiness by mimicking a failover from the protected site to the recovery site. This procedure is done without affecting application monitoring.

When you run a test recovery plan, the virtual machines specified in the plan appear in the isolated network at the recovery site.

For details, refer to, VMware product documentation.

For test recovery, Symantec recommends you to modify your network settings such that,

- The recovery site vCenter Server and Symantec High Availability Console is able to communicate with the test virtual machines.
- Create a dedicated network for the test virtual machines to failover. The target ESX console port should be accessible over this virtual network.
  To create this network, you must select "Auto" as the Test Network while you create the SRM Recovery Plan.
- Configure the test virtual machines such that they are accessible over the virtual network created.

Note: If you do not set up a dedicated network for the test virtual machines to failover, the virtual machines failover in an isolated network. During the failover the VMwareDisk agent successfully, deports and imports the VMware disk to the target virtual machine and the application dependency group is successfully brought online. However, the VMwaredisk agent goes in to an "Unknown" state.

Appendix B

Sample VCS_Site_Info.xml file

This appendix includes the following topics:

- Sample VCS_Site_Info.xml file

Sample VCS_Site_Info.xml file

The following sample xml depicts the VCS_Site_Info.xml file. This file lists the attribute values for the configured application components, on both the sites.

```
<SiteInfo>
<site name="SiteB">
<attr resname="GenericApplication-SG-Lanman"
attrname="VirtualName" type="scalar">
<value data="LanmanName_SiteB"/>
</attr>
<attr resname="GenericApplication-SG-VMWareDisks"
attrname="ESXDetails" type="assoc">
<value data="ESXIP_SiteB" rvalue="root=ESXPassword_encrypted
ByVCS_SiteB"/>
</attr>
<attr resname="GenericApplication-SG-IP" attrname="Address" type="scalar">
</attr>
</site>
<site name="SiteA">
<attr resname="GenericApplication-SG-Lanman"
attrname="VirtualName" type="scalar">
</attr>
<attr resname="GenericApplication-SG-VMWareDisks"
```

```
attrname="ESXDetails" type="assoc">
<value data="ESXIP_SiteA" rvalue="root=ESXPassword_encrypted
ByVCS_SiteA"/>
</attr>
<attr resname="GenericApplication-SG-IP" attrname="Address" type="scalar">
</attr>
</site>
</SiteInfo>
```

Appendix C

Troubleshooting

This appendix includes the following topics:

About error logging

The error log "server\log\healthview_A.txt " is generated for the errors that may occur while executing the application monitoring command step in the SRM recovery plan.

The log file is located at the following path on the virtual machine:

```
C:\Program Files\Veritas\cluster
```

All VCS cluster systems fail to start at the same time

In a SRM recovery plan, Symantec recommends to add all the VCS cluster systems under the same priority order. This ensures that all the virtual machines are started at the same time and the application dependency group is brought online successfully.

However, if due to any network issues all the VCS cluster systems do not start at the same time, then VCS cluster fails to start and the application monitoring continuity is lost.

Workaround: You must manually seed the VCS cluster.

For more details on seeding a cluster, refer to the *Veritas™ Cluster Server Administrator's Guide.*